

REMARKS

Claims 1-67 remain pending in the application. Reconsideration is respectfully requested in light of the following remarks.

Section 101 Rejection

The Examiner rejected claims 1-67 under 35 U.S.C. § 101 as being directed to non-statutory matter. In spite of the amendments made to many of the claims in Applicants' last Response, the Examiner merely repeats his assertion that the claimed invention is based on non-statutory matter and directed towards nothing more than the abstract idea of a mathematical algorithm. Applicants again traverse this rejection, and again note that claims 1 and 21, for example, have been amended to recite a method implemented in a device supporting a public-key cryptography application, wherein the device comprises multiple arithmetic *circuits* that perform various operations of the method, and to recite limitations involving the storage and subsequent use of a generated partial result in a public-key cryptography application. The other independent claims have been similarly amended.

Applicants remind the Examiner that, according to MPEP 2106.IV.C, "While abstract ideas, natural phenomena, and laws of nature are not eligible for patenting, methods and products employing abstract ideas, natural phenomena, and laws of nature to perform a real-world function may well be. In evaluating whether a claim meets the requirements of section 101, the claim must be considered as a whole to determine whether it is for a particular application of an abstract idea, natural phenomenon, or law of nature, and not for the abstract idea, natural phenomenon, or law of nature itself." In addition, MPEP 2106.02 states, "In practical terms, claims define nonstatutory processes if they consist solely of mathematical operations without some claimed practical application (i.e., executing a "mathematical algorithm")." Applicants assert that none of Applicants' claims consist solely of mathematical operations without some claimed practical application, nor are the mathematical operations recited therein performed in the

abstract. Rather, they are performed within a very specific practical context, i.e., in methods, processors, and apparatus supporting public-key cryptography applications. For example, methods (such as those of claims 1 and 21) implemented in a device supporting public-key cryptography that produce a generated partial result for use in a cryptography application are clearly directed to a claimed practical application. Similarly, processors (such as those of claims 38 and 53) that include structures for implementing various operations of a cryptography application are clearly not directed solely to mathematical operations, but are directed to real-world implementations that support a claimed practical application.

In addition, an apparatus configured to support a public-key cryptography application (as in claims 66 and 67) is clearly directed to a real-world implementation of acts performed within a specific practical application. Applicants further remind the Examiner that, according to MPEP 2106, “Where means plus function language is used to define the characteristics of a machine or manufacture invention, such language must be interpreted to read on only the structures or materials disclosed in the specification and “equivalents thereof” that correspond to the recited function. Two en banc decisions of the Federal Circuit have made clear that the USPTO is to interpret means plus function language according to 35 U.S.C. § 112, sixth paragraph. In *re Donaldson*, 16 F.3d 1189, 1193, 29 USPQ2d 1845, 1848 (Fed. Cir. 1994) (en banc); In *re Alappat*, 33 F.3d 1526, 1540, 31 USPQ2d 1545, 1554 (Fed. Cir. 1994) (en banc). Disclosure may be express, implicit, or inherent. Thus, at the outset, USPTO personnel must attempt to correlate claimed means to elements set forth in the written description that perform the recited step or function. The written description includes the original specification and the drawings and USPTO personnel are to give the claimed means plus function limitations their broadest reasonable interpretation consistent with all corresponding structures or materials described in the specification and their equivalents including the manner in which the claimed functions are performed. See *Kemco Sales, Inc. v. Control Papers Company, Inc.*, 208 F.3d 1352, 54 USPQ2d 1308 (Fed. Cir. 2000). Therefore, according to 35 U.S.C. 112 “An element in a claim for a combination may be expressed as a means or step for performing a specified function without the recital of structure, material, or

acts in support thereof, and such claim shall be construed to cover the corresponding structure, material, or acts described in the specification and equivalents thereof.” Applicants assert that the written description clearly includes read-world embodiments of the claimed invention, including various hardware and/or software elements that may implement the functionality recited.

The Examiner further notes that a claimed invention reciting a computer program product that solely calculates a mathematical formula or a computer readable medium that solely stores a mathematical formula is not directed to the type of subject matter eligible for patent protection. **The Examiner is incorrect.** Applicants note that while Applicants’ specification includes descriptions of processor instructions that may be implemented in a processor to support cryptography applications, none of the claims of the present invention recite merely *a computer program product*, as erroneously suggested by the Examiner. Applicants further remind the Examiner that, according to MPEP 2106.01, **a claimed computer-readable medium encoded with a computer program is a computer element which defines structural and functional interrelationships between the computer program and the rest of the computer which permit the computer program's functionality to be realized, and is thus statutory. See Lowry, 32 F.3d at 1583-84, 32 USPQ2d at 1035.**

For at least the reasons above, Applicants respectfully request removal of the rejection of claims 1-67 under 35 U.S.C. § 101.

Section 102(e) Rejection:

The Examiner rejected claims 1-10, 12-19, 21-29, 32-36, 38-46, 48-60 and 62-67 as being anticipated by Gressel et al. (U.S. Patent 6,748,410) (hereinafter “Gressel”). Applicants respectfully traverse this rejection for at least the following reasons.

Regarding claim 1, contrary to the Examiner’s assertion, Gressel fails to disclose all the limitations of this claim. The Examiner quotes the entire text of claim 1 and cites

a long list of passages in Gressel as teaching: feedback of a previous operation into next operation; arithmetic operation or instructions; arithmetic structure; multiplication two values, summing two values utilizing partial (i.e., bit operations, any bit length, high order bits, low order bits) results from previous multiplication; adder; carry-save adder; carry-out; register usage; XOR operations; redundant representation of numbers; acceleration, improvements of arithmetic operations; arithmetic operations utilized to generate cryptography key(s); and processor utilization for key generation. The Examiner submits that Gressel discloses all the limitations of claim 1, in its current form, in these passages, but does not relate the teachings of these passages to any of the specific limitations of claim 1. Instead, the Examiner merely points out general references to the elements listed above in the system of Gressel, many of which have nothing to do with the limitations recited in claim 1. **Therefore, Applicants again assert that the Examiner has failed to address each and every limitation of independent claim 1 in his remarks.** For example, the Examiner's remarks as to the teachings of the cited passages in Gressel do not address all of the specific limitations of claim 1, such as "generating a first partial result of a currently executing arithmetic instruction... the first partial result representing the high order bits summed with low order bits of a result of a first number multiplied by a second number." Instead, the Examiner submits that Gressel teaches, "multiplication two values, summing two values utilizing parallel (i.e., bit operations, any bit length, high order bits, low order bits) results from previous multiplication." **This is clearly not what is recited in claim 1, nor does it teach the limitations of claim 1.** Applicants again note MPEP 707.07(d), which requires that, in an Examiner's Action, the ground of rejection, should be "fully and clearly stated". **Since the rejection of claim 1 has not been fully and clearly stated, Applicants assert that it is improper.**

Further regarding claim 1, the Examiner equates adding a value of "any bit length" and generic references to "high order bits" and "low order bits" to the limitation, "generating a first partial result of a currently executing arithmetic instruction... the first partial result representing the high order bits summed with low order bits of a result of a first number multiplied by a second number." Applicants previously noted that the

Examiner's cited passage (Gressel, column 2, lines 31-37) states, in its entirety: "Further in accordance with a preferred embodiment of the present invention, the employing step includes multiplying a first integer of any bit length by a second integer of any bit length to obtain a first product, multiplying a third integer of any bit length by a fourth integer of any bit length to obtain a second product, and summing the first and second products with a fifth integer of any bit length to obtain a sum." Applicants noted that this passage describes nothing about "high order bits" or "low order bits" as suggested by the Examiner, nor about a partial result of a currently executing arithmetic instruction. **Furthermore, this description of multiplying (input) values of any bit length to obtain products and then adding the products together clearly does not teach the specific limitations of the first partial result recited claim 1, i.e., *the first partial result representing the high order bits summed with low order bits of a result of a first number multiplied by a second number*.** In addition, Applicants asserted that the cited passages do not teach the additional limitations, "storing the first partial result; and using the stored first partial result in a subsequent computation in the public-key cryptography application," as recited in claim 1.

In the Response to Arguments section of the Final Action, the Examiner disagrees with Applicants' argument above and submits, "The claim limitations merely recite arithmetic operations which are performed on integer values. The Gressel and Stribaek prior art combination discloses arithmetic operations performed on integer values. The stated types of operations indicated by the prior art discloses". Applicants again assert that the Examiner is ignoring the specific wording of Applicants' claims. As discussed above, they do not "merely recite arithmetic operations which are performed on integer values" as erroneously suggested by the Examiner. Instead, claim 1, for example, recites specific operations performed by various arithmetic circuits of a device to implement a portion of a cryptography application. Applicants remind the Examiner that "All words in a claim must be considered in judging the patentability of that claim against the prior art." MPEP 2143.03; *In re Wilson*, 424 F.2d 1382, 1385, 165 USPQ 494, 496 (CCPA 1970).

The Examiner submits that the Gressel prior art discloses the results of a first arithmetic operation used as input to another arithmetic operation (col. 3, lines 1-7; col. 53, lines 13-19; col. 53, lines 49-51). **Applicants note that this generic reference to “results of a first arithmetic operation used as input to another arithmetic operation” is not what is recited in Applicants’ claim.** The first of the Examiner’s cited passages describes collecting and serially summing multiplicands generated in a Montgomery multiplication to generate a sum and to feed in the sum to another Montgomery multiplication. **It teaches nothing about a partial result, much less one having all the limitations of the first partial result recited in claim 1.** The second and third of these citations describe the operation of a thirty-two bit shift register, which is configured as a non-linear feedback shift register. **They teach nothing about the specific limitations recited in claim 1.**

In the Response to Arguments section of the Final Action, the Examiner also submits, “A bit value of an arbitrary length is a partial result. The high order bits are a partial result. The low order bits are a partial result. The two partial results are combined by adding the products. This is equivalent to a first partial result representing the high order bits summed with the low order bits of a result of a first number multiplied by a second number.” **Applicants assert that this interpretation is completely unsupported by the cited art.** The Examiner’s citation regarding multiplying integers of any bit length describes nothing about these integers being partial results of other operations, nor about them comprising “high order bits” or “low order bits” as the Examiner suggests. Instead, they are merely described as “integers.” As previously noted, nothing in Gressel describes combining “high order bits” and “low order bits”, as the Examiner suggests, or a partial result of a currently executing arithmetic instruction, **much less the specific limitations recited in claim 1.**

In the Response to Arguments section of the Final Action, the Examiner submits, “The Gressel prior art discloses arithmetic operations such as multiplication and addition utilizing the partial results of the first operation.” Applicants again assert that the cited passages describe multiplication of integers, without any reference to utilizing partial

results of a previous operation, and general references to linear feedback shift registers. **These passages clearly are not sufficient to teach the specific limitations of claim 1.**

The Examiner includes remarks regarding VLIW architectures, and the fact that they specify multiple simultaneous operations in a single instruction. **These remarks have absolutely nothing to do with Applicants' claims.** Applicants assert that no one of ordinary skill in the art would consider a VLIW instruction to be the single arithmetic instruction as specifically recited in claim 1. Applicants also note that nothing in Gressel describes that it is (or could be) a VLIW architecture. In addition, in a VLIW architecture, the multiple operations specified by a single instruction are performed simultaneously. Therefore, by definition, none of the operations thereof can rely on feedback from other ones of the operations thereof. **Thus, a VLIW instruction clearly does not teach the single arithmetic instruction of Applicants' claim.**

Finally, the Examiner submits that Gressel teaches “storing and utilizing the results of an operation in subsequent arithmetic operations” in the passages cited above and in that “An instruction also designates the destination address (memory locations, registers) for the results of the completion of an instruction.” This generic reference to destination addresses teaches nothing about the specific limitations recited in claim 1 regarding a method that includes storing a first partial result (i.e., one having the limitations recited in Applicants' claim) and using this stored first partial result in a subsequent computation in a public-key cryptography application.

Applicants remind the Examiner that anticipation requires the presence in a single prior art reference disclosure of each and every element of the claimed invention, arranged as in the claim. *Lindemann Maschinenfabrik GmbH v. American Hoist & Derrick Co.*, 221 USPQ 481, 485 (Fed. Cir. 1984). The **identical invention must** be shown **in as complete detail** as is contained in the claims. *Richardson v. Suzuki Motor Co.*, 9 USPQ2d 1913, 1920 (Fed. Cir. 1989). As discussed above, is clear that Gressel does not teach the elements of Applicants' claim 1 as arranged in the claim and in as complete detail as in the claim, as required. **Applicants assert that the Examiner has**

merely picked and chosen individual disparate words, phrases, and elements of Applicants' claim that are found, or in some cases are not found, in the Gressel reference and attempted to piece them together in a manner not described in the cited art to reconstruct Applicants' claim. Applicants remind the Examiner that "It is impermissible. . . simply to engage in a hindsight reconstruction of the claimed invention, using the applicant's structure as a template and selecting elements from references to fill the gaps." *In re Gorman*, 933 F.2d 982, 987 (Fed. Cir. 1991). Therefore, Gressel cannot be said to anticipate claim 1.

For at least the reasons above, the rejection of claim 1 is unsupported by the cited art and removal thereof is respectfully requested.

Independent claims 38 and 66 include limitations similar to those of claim 1, and were rejected using remarks identical to those used in the rejection of claim 1. Therefore, the arguments presented above apply with equal force to these claims as well.

Regarding independent claim 21, the Examiner again quotes the entire text of claim 21 and cites the same long list of passages in Gressel, including the same remarks used to reject claim 1. Therefore, the arguments presented above apply with equal force to this claim, as well.

In addition, Applicants previously noted that claim 21 includes limitations different from those in claim 1 and that the Examiner has not specifically addressed these differences in his remarks. **The Examiner has again failed to address these limitations in the Final Action.** Therefore, the rejection of claim 21 is improper. For example, claim 21 includes the limitations "*supplying a third number to the second arithmetic circuit; the second arithmetic circuit generating a first partial result of a currently executing arithmetic instruction in the public-key cryptography application, the first partial result being a representation of the high order bits summed with low order bits of a result of a first number multiplied by a second number and with the third number, the summing being performed during multiplication of the first number and the second number, the summing and at least a portion of the multiplication being performed in the*

second arithmetic circuit.” Applicants again assert that the Examiner has cited nothing in cited art to teach these limitations, and that it does not teach these limitations. Therefore, Gressel cannot be said to anticipate claim 1.

For at least the reasons above, the rejection of claim 21 is unsupported by the cited art and removal thereof is respectfully requested.

Independent claims 53 and 67 include limitations similar to those of claim 21, and were rejected using remarks identical to those used in the rejection of claim 21. Therefore, the arguments presented above apply with equal force to these claims as well.

Regarding claim 2, contrary to the Examiner’s assertion, Gressel fails to disclose *wherein the high order bits are fed back in redundant number representation.* The Examiner cites a subset of the passages cited in remarks regarding claim 1. As discussed above, these citations do not teach the feedback of high order bits recited in Applicants’ claims. The Examiner cites column 29, lines 43-49 as teaching “redundant representation of numbers.” **This passage actually describes the use of a redundant register. It has absolutely nothing to do with redundant representation of numbers, as the Examiner suggests.** Therefore, Gressel cannot be said to anticipate claim 2.

For at least the reasons above, the rejection of claim 2 is unsupported by the cited art and removal thereof is respectfully requested.

Claim 35 includes limitations similar to those of claim 2, and so the arguments presented above apply with equal force to this claim as well.

Regarding claim 3, contrary to the Examiner’s assertion, Gressel fails to disclose *wherein the redundant number representation includes sum and carry bits.* The Examiner again cites a subset of the passages cited in remarks regarding claim 1, including column 29, lines 43-49 as teaching “redundant representation of numbers.” **However, this passage actually describes the use of a redundant register. It has absolutely nothing to do with redundant representation of numbers, as the**

Examiner suggests, no matter what such a redundant representation includes. Therefore, Gressel cannot be said to anticipate claim 3.

For at least the reasons above, the rejection of claim 3 is unsupported by the cited art and removal thereof is respectfully requested.

Regarding claim 4, contrary to the Examiner's assertion, Gressel fails to disclose *feeding back the high order bits through a register to the second arithmetic circuit*. The Examiner again cites a subset of the passages cited in remarks regarding claim 1. As discussed above, these citations do not teach the feedback of high order bits recited in Applicants' claim 1, nor the use of a register for this specific purpose. Therefore, Gressel cannot be said to anticipate claim 4.

For at least the reasons above, the rejection of claim 4 is unsupported by the cited art and removal thereof is respectfully requested.

Claims 22, 42, and 57 include limitations similar to those of claim 4, and so the arguments presented above apply with equal force to these claims as well.

Regarding claim 5, contrary to the Examiner's assertion, Gressel fails to disclose *generating a second partial result of the currently executing arithmetic instruction in the first arithmetic circuit, the second partial result representing the high order bits of the multiplication result of the first number multiplied by the second number*. The Examiner again cites a subset of the passages cited in remarks regarding claim 1. These passages describe various arithmetic operations, but not the specific limitations of Applicants' claim. For example, just as they do not teach the first partial result recited in claim 1, they also do not teach the second partial result of claim 5, according to the specific limitations recited, e.g., the second partial result representing the high order bits of the multiplication result of the first number multiplied by the second number. Applicants again assert that Gressel does not teach these elements as arranged in the claim. Therefore, Gressel cannot be said to anticipate claim 5.

For at least the reasons above, the rejection of claim 5 is unsupported by the cited art and removal thereof is respectfully requested.

Claims 23, 39, and 54 include limitations similar to those of claim 5, and so the arguments presented above apply with equal force to these claims as well.

Regarding claim 6, contrary to the Examiner's assertion, Gressel fails to disclose *generating a second partial result of the currently executing arithmetic instruction, the second partial result representing the high order bits of the multiplication result of the first number multiplied by the second number summed with the high order bits of the previously executed arithmetic instruction*. The Examiner again cites a subset of the passages cited in remarks regarding claim 1. These passages describe various arithmetic operations, but not the specific limitations of Applicants' claim. For example, just as they do not teach the first partial result recited in claim 1, they also do not teach the second partial result of claim 5, according to the specific limitations recited, e.g., the second partial result representing the high order bits of the multiplication result of the first number multiplied by the second number summed with the high order bits of the previously executed arithmetic instruction. Applicants again assert that Gressel does not teach these elements as arranged in the claim. Therefore, Gressel cannot be said to anticipate claim 6.

For at least the reasons above, the rejection of claim 6 is unsupported by the cited art and removal thereof is respectfully requested.

Claim 24 includes limitations similar to those of claim 6, and so the arguments presented above apply with equal force to this claim as well.

Regarding claim 7, contrary to the Examiner's assertion, Gressel fails to disclose *supplying values generated in one or more most significant columns of the second arithmetic structures to one or more least significant columns of the first arithmetic structures while generating the first and second partial results*. The Examiner again cites a subset of the passages cited in remarks regarding claim 1, including col. 31, lines 44-46

and col. 41, lines 3-5 “arithmetic structure.” These passages describe that the system of Gressel employs the standard structure of a serial/parallel multiplier as the basis for constructing a double acting serial parallel multiplier. The other cited passages include general reference to linear feedback shift registers and arithmetic instructions, but teach nothing about the specific limitations of claim 7, involving *supplying values generated in one or more most significant columns of the second arithmetic structures to one or more least significant columns of the first arithmetic structures while generating the first and second partial results, as arranged in the claim.* Therefore, Gressel cannot be said to anticipate claim 7.

For at least the reasons above, the rejection of claim 7 is unsupported by the cited art and removal thereof is respectfully requested.

Claims 25, 40, and 55 include limitations similar to those of claim 7, and so the arguments presented above apply with equal force to these claims as well.

Regarding claim 8, contrary to the Examiner’s assertion, Gressel fails to disclose *wherein the generating of the first and second partial result is in response to execution of a single arithmetic instruction.* The Examiner again cites a subset of the passages cited in remarks regarding claim 1, including three passages that he submits teach “arithmetic operation or instruction.” Two of these passages refer to a goal to provide “large integer arithmetic” and the third refers to, “a device that can implement modular multiplication/exponentiation of large numbers.” None of these passages, or anything else in Gressel teaches that the generating of the first and second partial results (those defined as recited in claims 1 and 5) is in response to execution of a single arithmetic instruction. Therefore, Gressel cannot be said to anticipate claim 8.

For at least the reasons above, the rejection of claim 8 is unsupported by the cited art and removal thereof is respectfully requested.

Claims 26, 41, and 56 include limitations similar to those of claim 8, and so the arguments presented above apply with equal force to these claims as well.

Regarding claim 9, contrary to the Examiner's assertion, Gressel fails to disclose *wherein the generating of the first and second partial result is in response to execution of a single arithmetic instruction*. The Examiner again cites a subset of the passages cited in remarks regarding claim 1, including three passages that he submits teach "arithmetic operation or instruction." Two of these passages refer to a goal to provide "large integer arithmetic" and the third refers to, "a device that can implement modular multiplication/exponentiation of large numbers." None of these passages, or anything else in Gressel teaches that the generating of the first and second partial results (those defined as recited in claims 1 and 6) is in response to execution of a single arithmetic instruction. Therefore, Gressel cannot be said to anticipate claim 9.

For at least the reasons above, the rejection of claim 9 is unsupported by the cited art and removal thereof is respectfully requested.

Regarding claim 13, contrary to the Examiner's assertion, Gressel fails to disclose *a logical circuit in at least one of the first and second arithmetic circuits supplying a fixed value if in XOR multiplication mode or a variable value that varies according to inputs supplied to the logical circuit if in integer multiplication mode, to thereby ensure a result is determined in XOR multiplication unaffected by carry logic performing carries in integer multiplication mode*. The Examiner again cites a subset of the passages cited in remarks regarding claim 1, two of which he cites as teaching "XOR operations". One of these citations states, "These five values are XORed together to produce the next Y_0 bit, Y_{0i} " and the other states, "the thirty two bit shift register with the four XORed feedbacks, is configured as a $n=32$ bit non-linear de Bruijn maximum length non-linear feedback shift register." **While these passages include the term "XOR" they have nothing to do with Applicants' claim.** Nothing in the cited passages or elsewhere in Gressel discloses an arithmetic circuit having an XOR multiplication mode and an integer multiplication mode, or such a circuit supplying different values (e.g., a fixed value or a variable value) depending on the mode, as in claim 13. Therefore, Gressel cannot be said to anticipate claim 13.

For at least the reasons above, the rejection of claim 13 is unsupported by the cited art and removal thereof is respectfully requested.

Claims 33, 50, and 64 include limitations similar to those of claim 13, and so the arguments presented above apply with equal force to these claims as well.

Regarding claim 14, contrary to the Examiner's assertion, Gressel fails to disclose *wherein the logical circuit operates as a majority circuit in integer multiplication mode and outputs a zero in the XOR multiplication mode*. The Examiner cites a different subset of the passages cited in remarks regarding claim 1 than those included in his remarks regarding claim 13, but includes the same two citations as teaching "XOR operations". **While these passages include the term "XOR" they have nothing to do with Applicants' claim.** Nothing in the cited passages or elsewhere in Gressel discloses a logical circuit having an XOR multiplication mode and an integer multiplication mode, or such a circuit operating as a majority circuit in integer multiplication mode and outputting a zero in XOR multiplication mode, as in claim 14. Therefore, Gressel cannot be said to anticipate claim 14.

For at least the reasons above, the rejection of claim 14 is unsupported by the cited art and removal thereof is respectfully requested.

Claims 34, 51, and 65 include limitations similar to those of claim 14, and so the arguments presented above apply with equal force to these claims as well.

Regarding claim 15, contrary to the Examiner's assertion, Gressel fails to disclose *wherein the first partial result is in redundant number representation*. The Examiner again cites a subset of the passages cited in remarks regarding claim 1. As discussed above, these citations do not teach the first partial result recited in Applicants' claims. The Examiner also again cites column 29, lines 43-49 as teaching "redundant representation of numbers." **As noted above, this passage describes the use of a redundant register. It has absolutely nothing to do with redundant representation**

of numbers, as the Examiner suggests. Therefore, Gressel cannot be said to anticipate claim 15.

For at least the reasons above, the rejection of claim 15 is unsupported by the cited art and removal thereof is respectfully requested.

Claim 43 includes limitations similar to those of claim 15, and so the arguments presented above apply with equal force to these claims as well.

Regarding claim 19, contrary to the Examiner's assertion, Gressel fails to disclose *feeding back high order bits of the currently executing arithmetic instruction from the first arithmetic circuit to the second arithmetic circuit for use with execution of a subsequent single arithmetic instruction.* The Examiner again cites a subset of the passages cited in remarks regarding claim 1, including three passages that he submits teach "arithmetic operation or instruction." As previously noted, two of these passages refer to a goal to provide "large integer arithmetic" and the third refers to, "a device that can implement modular multiplication/exponentiation of large numbers." None of these passages, or anything else in Gressel teaches feeding back high order bits... for use with execution of a subsequent single arithmetic instruction. Therefore, Gressel cannot be said to anticipate claim 19.

For at least the reasons above, the rejection of claim 19 is unsupported by the cited art and removal thereof is respectfully requested.

Claim 36 includes limitations similar to those of claim 19, and so the arguments presented above apply with equal force to this claim as well.

Section 103 Rejection:

The Examiner rejected claims 11, 20, 30, 31, 37, 47 and 61 under 35 U.S.C. § 103(a) as being unpatentable over Gressel et al. (US Patent No. 6,748,410) (hereinafter

“Gressel”) in view of Stribaek et al. (US Patent No. 6,181,484). Applicants respectfully traverse this rejection for at least the following reasons.

Regarding claim 11, contrary to the Examiner’s assertion, Gressel in view of Stribaek fails to teach or suggest *wherein at least one of the first and second pluralities of arithmetic structures comprises a plurality of Wallace tree columns*. The Examiner first states, “Gressel discloses the method as recited in claim 1 wherein at least one of the first and second pluralities of arithmetic structures comprises a plurality of Wallace tree columns” and then states, “Gressel does not specifically disclose whereby a plurality of Wallace tree columns. However Stribaek discloses wherein further comprises a plurality of Wallace tree columns. (see Stribaek col. 9, lines 10-24; col. 9, lines 37-39: Wallace tree.)” Applicants again assert that Gressel does not teach the limitations of claim 1, as discussed above. Therefore, for at least the reasons above, the rejection of claim 11, which depends from claim 1, is unsupported by the cited art. In addition, the Examiner’s conflicting statements about whether or not Gressel discloses the limitations of claim 11 render this rejection improper.

In Stribaek, microprocessor instructions are provided for manipulating portions of an extended precision accumulator including instructions to move the contents of a portion of the extended accumulator to a general-purpose register and instructions to move the contents of a general-purpose register to a portion of the extended accumulator (see, e.g., Stribaek Abstract, and descriptions of the instructions MFHI, MFLO, MTHI, MTLO, MFLHXU, and MTLHX). Stribaek’s system also includes a 32-bit by 16-bit Wallace tree multiplier array that has been modified to support the addition of two 72-bit wide operands ACC1 and ACC2. However, Stribaek (taken alone or in combination with Gressel) does not teach or suggest the specific limitations of Applicants’ claimed invention, in which at least one of the two arithmetic structures recited in claim 1 (the first and second arithmetic units) comprise a plurality of Wallace tree columns and operate according to the specific limitations of claim 1. The mere addition of a Wallace tree multiplier array to the system of Gressel would not necessarily result in the invention of claim 11. As discussed above, Gressel does not teach all the limitations recited in

claim 1. Applicants assert that Stribaek does not overcome the deficiencies of Gressel in teaching them, and the Examiner has not relied on Stribaek to teach them. Therefore, the combination of the references cannot teach all the limitations of claim 11.

The Examiner submits that it would have been obvious to one of ordinary skill in the art to modify Gressel as taught by Stribaek to enable the capability for the usage of Wallace tree multiplication, and that one of ordinary skill in the art would have been motivated to employ the teachings of Stribaek in order to enable the capability for extended precision in arithmetic calculations due to extensive and increasing use of public key cryptography (citing Stribaek, column 1, lines 61-67). Applicants assert, however, that the system of Gressel already employs multiprecision modular multiplication methods for large operand integer arithmetic used in cryptography computations, including in public key cryptography (see, e.g., col. 3, lines 24-45). Therefore, there would be no reason for the skilled artisan to employ different structures for these purposes.

Applicants respectfully remind the Examiner that to establish a *prima facie* obviousness of a claimed invention, all claim limitations must be taught or suggested by the prior art. *In re Royka*, 490 F.2d 981, 180 U.S.P.Q. 580 (C.C.P.A. 1974), MPEP 2143.03. The cited art, taken alone or in combination, does not teach or suggest all limitations of claim 11, as discussed above.

For at least the reasons above, the rejection of claim 11 is unsupported by the cited art and removal thereof is respectfully requested.

Claims 30, 47, and 61 include limitations similar to those of claim 11, and so the arguments presented above apply with equal force to these claims as well.

In regard to the rejections under both § 102(e) and § 103(a), Applicants also assert that numerous ones of the dependent claims recite further distinctions over the cited art. However, since the rejections have been shown to be unsupported for the independent claims, a further discussion of the dependent claims is not necessary at this time.

CONCLUSION

Applicants submit the application is in condition for allowance, and notice to that effect is respectfully requested.

If any fees are due, the Commissioner is authorized to charge said fees to Meyertons, Hood, Kivlin, Kowert, & Goetzel, P.C. Deposit Account No. 501505/6000-31500/RCK.

Respectfully submitted,

/Robert C. Kowert/

Robert C. Kowert, Reg. #39,255
Attorney for Applicants

Meyertons, Hood, Kivlin, Kowert, & Goetzel, P.C.
P.O. Box 398
Austin, TX 78767-0398
Phone: (512) 853-8850

Date: January 28, 2008